

On Improving 4×4 Space-Time Codes

Frédérique Oggier
Department of Electrical Engineering
California Institute of Technology
91125 Pasadena, CA.
Email: frederique@systems.caltech.edu

Grégory Berhuy
School of Mathematics
University of Southampton
Southampton, SO17 1BJ U.K.
Email: G.W.Berhuy@soton.ac.uk

Abstract—In this work, we discuss the construction of 4×4 space-time codes for coherent MIMO channels. Recently, the so-called perfect space-time codes have been introduced. These are algebraic codes, which satisfy a plethora of properties, that makes them particularly efficient. They are available for 2,3,4 and 6 antennas, and the optimal perfect code for 2 antennas is known. In an attempt to find the optimal perfect code for 4 antennas, we found and present here a (non perfect) code construction that exhibits better performance than 4×4 known codes.

I. INTRODUCTION

We consider the problem of coding over a coherent MIMO channel. In such a scenario, perfect codes have been introduced [2]. These are algebraic space-time codes, that have been proved to have a plethora of properties: they have full rate, in the sense that, for $M \oplus M$ codewords, the M^2 degrees of freedom are used to transmit M^2 information symbols. They have discrete determinants (the minimum determinant of the code does not decrease when increasing the spectral efficiency) and full diversity. They thus fulfill the two main design criteria for coherent space-time coding, namely the *diversity* and the *coding gain* given by the minimum determinant [6]. More recently, the asymptotic behavior of coherent space-time codes has been characterized by the diversity multiplexing trade off of Zheng and Tse [7]. Perfect space-time codes have been shown to reach the diversity multiplexing barrier of Zheng Tse [1]. They also benefit of an efficient encoding, which consists in putting the information symbols into the layer of the space-time code using a lattice structure, that does not increase the energy of the system. This property is also called information lossless [5], and guarantees that there is no loss of capacity compared to uncoded systems.

Because they satisfy a large number of constraints, perfect codes are difficult to construct [2]. Thus the question of the optimality of the existing ones has been addressed only recently [3], and a proof of optimality is available only for 2 antennas. The construction that will be presented in this paper was found while trying to find the optimal perfect code for 4 antennas. It was shown in [3] that the main parameter to be improved is actually the coding gain, which can be expressed in closed form while considering those algebraic

codes. It appeared that trying to reduce the coding gain very often contradicts the fully diversity property, in the sense that there exists at least a pair of codewords $\mathbf{X} \neq \mathbf{X}'$ such that $\det(\mathbf{X} \oplus \mathbf{X}') = 0$. This motivates the following questions: if the event that there exists a pair of codewords $\mathbf{X} \neq \mathbf{X}'$ such that $\det(\mathbf{X} \oplus \mathbf{X}') = 0$ is marginal, how does it affect the performance of the code? Can we get a substantial coding gain by slightly relaxing the full diversity constraint and allowing marginally the rank of the difference of two codewords to decrease?

This paper is organized as follows: we first start by recalling how algebraic codes are built using cyclic algebras. We then give a code construction which improves significantly in terms of coding gain, though marginally allows for non full-diversity. We then show simulation results and conclude by a small discussion.

II. SPACE-TIME CODES BUILT ON CYCLIC ALGEBRAS

Cyclic algebras are non-commutative algebras. Those algebraic objects have been introduced as a tool for space-time coding in [4], and became popular since they naturally provide for linear fully-diverse codes. For general definitions and results, we let the reader refer to [4], [2].

A. Cyclic algebras

Since we are interested in a 4 antennas code, we recall the code construction and the basic definitions in dimension 4.

Let $\mathbb{Q}(i)$ be the set of complex numbers defined by

$$\mathbb{Q}(i) = \{b_0 + b_1 i \mid b_0, b_1 \in \mathbb{Q}\}.$$

Let $\gamma \in \mathbb{C}$ such that $\gamma^4 \in \mathbb{Q}(i)$ and $1, \gamma, \gamma^2, \gamma^3$ are linearly independent over $\mathbb{Q}(i)$. For such a γ , we set

$$\mathbb{Q}(\gamma) = \{a_0 + a_1 \gamma + a_2 \gamma^2 + a_3 \gamma^3 \mid a_j \in \mathbb{Q}(i)\}.$$

In particular, $\mathbb{Q}(\gamma)$ is a vector space of dimension 4 over $\mathbb{Q}(i)$, with basis $\{1, \gamma, \gamma^2, \gamma^3\}$. Furthermore, the $\mathbb{Q}(i)$ -linear map $\gamma : \mathbb{Q}(\gamma) \rightarrow \mathbb{Q}(\gamma)$ defined by

$$\gamma(\gamma^k) = i^k \gamma^k, \quad k = 0, \dots, 3$$

satisfies $\gamma^2 \neq \text{Id}$ and $\gamma^4 = \text{Id}$. The set $\{\gamma^j, j = 1, \dots, 4\}$ is a group called *the Galois group*. It is *cyclic* with 4 elements, with generator γ , since $\gamma^2 \neq \text{Id}$ and $\gamma^4 = \text{Id}$.

In view of these properties, we say that $\mathbb{Q}(\gamma)/\mathbb{Q}(i)$ is cyclic.

¹This work was supported in part by the Nuffield Newly Appointed Lecturers Scheme 2006 NAL/32706 and by the Swiss National Science Foundation grant PBEL2-110209, by the NSF grant CCR-0133818, by Caltech's Lee Center for Advanced Networking, by a grant from the David and Lucille Packard Foundation.

In the following, we set $L = \mathbb{Q}(\gamma)$. We construct a non-commutative algebra, denoted by $\mathcal{A} = (L/\mathbb{Q}(i), \gamma, \gamma)$, as follows:

$$\mathcal{A} = L \oplus eL \oplus e^2L \oplus e^3L,$$

where $\gamma \in \mathbb{Q}(i)$, and e satisfies

$$e^4 = \gamma \quad \text{and} \quad \gamma e = e\gamma(\gamma) \text{ for all } \gamma \in L.$$

Such an algebra is called a *cyclic algebra*.

Cyclic algebras have been considered for coding applications since they naturally provide families of matrices. Since each $x \in \mathcal{A}$ is expressible as

$$x = x_0 + ex_1 + e^2x_2 + e^3x_3, \quad x_i \in L \text{ for all } i,$$

there is a correspondence between $x \in \mathcal{A}$ and the matrix of multiplication by x given by

$$\begin{pmatrix} x_0 & \gamma\gamma(x_3) & \gamma\gamma^2(x_2) & \gamma\gamma^3(x_1) \\ x_1 & \gamma(x_0) & \gamma\gamma^2(x_3) & \gamma\gamma^3(x_2) \\ x_2 & \gamma(x_1) & \gamma^2(x_0) & \gamma\gamma^3(x_3) \\ x_3 & \gamma(x_2) & \gamma^2(x_1) & \gamma^3(x_0) \end{pmatrix}. \quad (1)$$

Indeed, let us compute the multiplication by x of any element $y \in \mathcal{A}$.

$$\begin{aligned} xy &= (x_0 + ex_1 + e^2x_2 + e^3x_3)(y_0 + ey_1 + e^2y_2 + e^3y_3) \\ &= x_0y_0 + e\gamma(x_0)y_1 + e^2\gamma^2(x_0)y_2 + \gamma^3(x_0)e^3y_3 \\ &\quad + ex_1y_0 + e^2\gamma(x_1)y_1 + e^3\gamma^2(x_1)y_2 + \gamma\gamma^3(x_1)y_3 \\ &\quad + e^2x_2y_0 + e^3\gamma(x_2)y_1 + \gamma\gamma^2(x_2)y_2 + e\gamma\gamma^3(x_2)y_3 \\ &\quad + e^3x_3y_0 + \gamma\gamma(x_3)y_1 + e\gamma\gamma^2(x_3)y_2 + e^2\gamma\gamma^3(x_3)y_3 \end{aligned}$$

since $e^4 = \gamma$ and using the noncommutativity rule $\gamma e = e\gamma(\gamma)$. In matrix form in the basis $\{1, e, e^2, e^3\}$, this yields

$$xy = \begin{pmatrix} x_0 & \gamma\gamma(x_3) & \gamma\gamma^2(x_2) & \gamma\gamma^3(x_1) \\ x_1 & \gamma(x_0) & \gamma\gamma^2(x_3) & \gamma\gamma^3(x_2) \\ x_2 & \gamma(x_1) & \gamma^2(x_0) & \gamma\gamma^3(x_3) \\ x_3 & \gamma(x_2) & \gamma^2(x_1) & \gamma^3(x_0) \end{pmatrix} \begin{pmatrix} y_0 \\ y_1 \\ y_2 \\ y_3 \end{pmatrix}.$$

There is thus a correspondence

$$x = x_0 + ex_1 + e^2x_2 + e^3x_3 \in \mathcal{A} \leftrightarrow \text{matrix (1)}$$

We denote by \mathbf{X} a codeword in the codebook \mathcal{C} which has the form of (1).

B. Encoding

Recall that each x_j in the matrix (1) is in L , thus of the form

$$x_j = \sum_{k=1}^4 a_{jk}\gamma^{k-1},$$

and similarly for $\gamma(x_j)$

$$\gamma(x_j) = \sum_{k=1}^4 a_{jk}\gamma(\gamma^{k-1}),$$

and the other powers of γ .

Thus every layer of the codeword (that is, any “diagonal” of the matrix (1)) can be written as

$$\begin{pmatrix} 1 & \gamma & \gamma^2 & \gamma^3 \\ 1 & \gamma(\gamma) & \gamma(\gamma^2) & \gamma(\gamma^3) \\ 1 & \gamma^2(\gamma) & \gamma^2(\gamma^2) & \gamma^2(\gamma^3) \\ 1 & \gamma^3(\gamma) & \gamma^3(\gamma^2) & \gamma^3(\gamma^3) \end{pmatrix} \begin{pmatrix} a_{j1} \\ a_{j2} \\ a_{j3} \\ a_{j4} \end{pmatrix} = \begin{pmatrix} x_j \\ \gamma(x_j) \\ \gamma^2(x_j) \\ \gamma^3(x_j) \end{pmatrix}$$

up to a multiplication by γ . Note that Q -QAM symbols can be seen as a subset of $\mathbb{Q}(i)$. Thus the encoding can be summarized as

$$\mathbf{X} = \sum_{j=1}^4 \text{diag}(R\mathbf{a}_j)\Gamma^{j-1},$$

where R is the above matrix, $\mathbf{a}_j = (a_{j1}, a_{j2}, a_{j3}, a_{j4})$, $j = 1, \dots, 4$ contains the information symbols, and

$$\Gamma = \begin{pmatrix} 0 & 0 & 0 & \gamma \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

Note that in order to have *information lossless code* [5], the matrix R has to be unitary and γ of complex modulus 1. In other words, those conditions also guarantee an efficient encoding, since the encoding does not change the energy at the transmitter.

C. Diversity and minimum determinant

The codebook \mathcal{C} made of matrices of the form (1) is linear (since γ is). Thus the rank criterion

$$\det(\mathbf{X} \oplus \mathbf{X}') \neq 0, \text{ for all } \mathbf{X} \neq \mathbf{X}' \in \mathcal{C},$$

simplifies to

$$\det(\mathbf{X}), \quad \mathbf{0} \neq \mathbf{X} \in \mathcal{C},$$

and the minimum determinant to

$$\min_{\mathbf{X} \neq \mathbf{0}} |\det(\mathbf{X})|^2, \quad \mathbf{X} \in \mathcal{C}.$$

It has been shown in [2] that the minimum determinant of codes built as described above is given by the following closed form expression

$$\frac{1}{|d_{L/\mathbb{Q}(i)}|}$$

where $d_{L/\mathbb{Q}(i)}$ is the so-called *discriminant* of $L/\mathbb{Q}(i)$ [2].

Clearly, the smallest the discriminant is, the better the coding gain is.

III. THE CODE CONSTRUCTION

In this work, we focus on optimizing the coding gain of the code, that is in finding L such that $L/\mathbb{Q}(i)$ has the smallest discriminant, while allowing for information lossless codes (that is, L has to be such that the unitary matrix R exists). We skip here the algebraic techniques that we use to find cyclic extensions $L/\mathbb{Q}(i)$ with small discriminants $d_{L/\mathbb{Q}(i)}$.

We propose the following construction. Let $\gamma = \exp(2\gamma i/16)$ be a primitive 16th root of unity. We have that

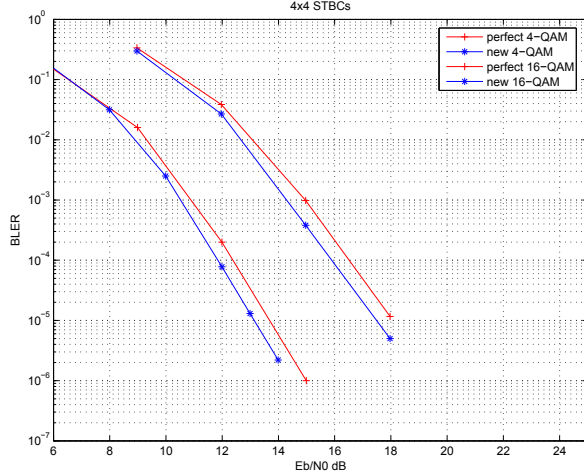


Fig. 1. Comparing the best previous known perfect code.

$\gamma^4 = i \in \mathbb{Q}(i)$ and $1, \gamma, \gamma^2, \gamma^3$ are linearly independent over $\mathbb{Q}(i)$. Therefore, we may consider $L = \mathbb{Q}(\gamma)$.

The corresponding map γ satisfies

$$\gamma(\gamma^k) = (i\gamma)^k = \gamma^{5k}.$$

Let R be the following unitary matrix:

$$R = \frac{1}{2} \begin{pmatrix} 1 & \gamma & \gamma^2 & \gamma^3 \\ 1 & \gamma(\gamma) & \gamma(\gamma^2) & \gamma(\gamma^3) \\ 1 & \gamma^2(\gamma) & \gamma^2(\gamma^2) & \gamma^2(\gamma^3) \\ 1 & \gamma^3(\gamma) & \gamma^3(\gamma^2) & \gamma^3(\gamma^3) \end{pmatrix}. \quad (2)$$

A codeword $\mathbf{X} \in \mathcal{C}'$ is given by

$$\mathbf{X} = \sum_{i=1}^4 \text{diag}(R\mathbf{a}_i)\Gamma^{i-1},$$

where $\mathbf{a}_i = (a_{i1}, a_{i2}, a_{i3}, a_{i4})$, $i = 1, \dots, 4$ contains the information symbols (from a Q -QAM constellation), and

$$\Gamma = \begin{pmatrix} 0 & 0 & 0 & i \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

Since it can be shown that $|d_{L/\mathbb{Q}(i)}| = 256$, we have that the new code \mathcal{C}' has a minimum nonzero determinant of

$$\gamma_{\min}(\mathcal{C}') = \frac{1}{256}.$$

It is however not true that this code is fully-diverse.

IV. SIMULATION RESULTS AND DISCUSSION

Performance of the code is illustrated in Fig. 1, where the new code has been simulated, for 4-QAM and 16-QAM constellations. It is surprising to notice that this codes does exhibit full diversity. The new code achieves a better coding gain, than for example here the known perfect code of [2],

which is what it was optimized for. Indeed, the known $4 \oplus 4$ perfect code \mathcal{C} in [2] achieves a minimum determinant of

$$\gamma_{\min}(\mathcal{C}) = \frac{1}{1125},$$

while the new code \mathcal{C}' has a minimum nonzero determinant of

$$\gamma_{\min}(\mathcal{C}') = \frac{1}{256}.$$

The new code also performs better than the best known previous codes presented in [2].

The explanation for this phenomenon is that though some pairs of codewords in the codebook have a difference whose rank decreases, the probability of getting this pair is very small, small enough to prevent the deterioration of the performance. It would be of interest to understand better this behavior, in particular to find a way of quantifying which proportion of pairs of matrices whose difference loses rank is required to influence the slope of the probability of error.

V. FUTURE WORK

There is still work to do to determine what are the optimal space-time codes for $4 \oplus 4$ MIMO channels, and in particular the optimal perfect space-time code. The code construction presented here addresses another type of question: can we reformulate the full-diversity criterion and determine which proportion of the pairs of codewords is allowed to drop rank without deteriorating the performance of the code?

REFERENCES

- [1] P. Elia, K. Raj Kumar, S. A. Pawar, P. Vijay Kumar and H.-F. Lu, "Explicit, Minimum-Delay Space-Time Codes Achieving The Diversity-Multiplexing Gain Tradeoff," *IEEE Trans. Inform. Theory*, vol. 52, no. 9, September 2006.
- [2] F. E. Oggier, G. Rekaya, J.-C. Belfiore and E. Viterbo, "Perfect Space-Time Block Codes", *IEEE Trans. on Information Theory*, vol. 52, no. 9, September 2006.
- [3] F. Oggier, "On the Optimality of the Golden Code", in the proceedings of the *Information Theory Workshop (ITW) 2006*, Chengdu.
- [4] B. A. Sethuraman, B. S. Rajan, and V. Shashidhar, "Full-diversity, high-rate space-time block codes from division algebras," *IEEE Trans. Inform. Theory*, vol. 49, pp. 2596–2616, October 2003.
- [5] V. Shashidhar, B. Sundar Rajan and B. A. Sethuraman, "Information-Lossless Space-Time Block Codes from Crossed-Product Algebras", *IEEE Trans. on Information Theory*, vol. 52, no. 9, September 2006.
- [6] V. Tarokh, N. Seshadri, and A. Calderbank, "Space-time codes for high data rate wireless communication : Performance criterion and code construction," *IEEE Trans. Inform. Theory*, vol. 44, pp. 744–765, March 1998.
- [7] L. Zheng, D. Tse, "Diversity and Multiplexing: A Fundamental Tradeoff in Multiple-Antenna Channels," *IEEE Trans. on Information Theory*, vol. 49, no. 5, pp. 1073–1096, May 2003.